



TENNESSEE INFORMATION PROTECTION ACT (TIPA)

CHECKLIST



USERCENTRICS

Tennessee Information Protection Act (TIPA) gives Tennessee residents rights over how their personal data is collected and used.

This checklist walks through steps that support your compliance efforts under the Act, along with recommended best practices for privacy-related user experience.



Important to know:

Action	Date
Effective date	July 1, 2025
Retroactive	No
Cure period	60 days, permanent

Note: TIPA offers an affirmative defense to businesses that create and maintain a written privacy program conforming to the NIST Privacy Framework. This is a protection not currently offered by other state privacy laws.

1 Determine If Your Company Is Required to Comply

If your for-profit organization:

- Exceeds USD 25 million in revenue, and
- Controls or processes the personal information of at least 25,000 Tennessee consumers, and derives more than 50 percent of gross revenue from the sale of personal information, or
- Controls or processes the personal information of at least 175,000 Tennessee residents during a calendar year

Entity-level exemptions:

- State government entities and political subdivisions
- [GLBA](#)-regulated financial institutions and affiliates
- Insurance companies licensed under Tennessee law
- [HIPAA](#)/HITECH-covered entities and business associates
- Nonprofit organizations
- Higher education institutions

Data-Level Exemptions:

- HR data, health records, and human-subjects research data
- Employment-related data
- Data created for or collected under several federal laws, including, among others:
 - HIPAA
 - Health Information Technology for Economic and Clinical Health Act
 - Health Care Quality Improvement Act and Patient Safety and Quality Improvement Act
 - [FCRA](#)
 - [COPPA](#)
 - FERPA
 - Driver's Privacy Protection Act
 - Farm Credit Act
 - Controlled Substances Act

2 Create a Comprehensive Privacy Policy

Upon receipt of an authenticated consumer request, businesses are required to provide a clear and accessible privacy notice that includes:

- Categories of personal data processed
- Purposes for which data is processed
- Categories of personal data the controller shares with third parties, if any
- Categories of third parties the controller shares personal data with, if any
- Third parties to whom the controller sells personal data or processes it for targeted advertising

Rights: Inform website visitors of their privacy rights and how to exercise them, including how to appeal a controller's decision.

Language: Keep the privacy policy clear and easy to understand.

Implementation: As a best practice, pair the privacy notice with an opt-out mechanism. For example, use a banner or popup when visitors visit your site, [powered by a CMP](#).

3 Inform Consumers About Their Rights

Consumers' rights under the TIPA:

- **Right to access:** Request and receive a copy of their personal data
- **Right to disclosure:** Categories of information about the consumer that have been sold
- **Right to correction:** Updates or corrections to inaccuracies in personal data collected
- **Right to deletion:** Personal data that has been collected about them (with exceptions)

- **Right to data portability:** Copy of personal data must be provided in a portable and readily useable format
- **Right to opt out:** Of processing of personal data for the purposes of sale, targeted advertising, or profiling
- **Right to nondiscrimination:** For exercising privacy rights
- **Right of minors:** Consent must be obtained from a parent or guardian before children's (under age 13) personal data is collected
- **Right to restrict sensitive personal information:** Limit or refuse the collection or use of personal data the law classifies as sensitive

4 As a Best Practice, Review and Update Your Privacy Policy Every 12 Months

Review your operations and any changes in the law every 12 months. Update the [privacy policy](#) and its effective date, even if no other changes are made.

Transparency: Keep the information visitors must be notified about clear, comprehensive, and up to date, with the last-update date clearly visible. A [Privacy Policy Generator](#) can help.

Data sold: List all categories of personal information your business has sold in the past 12 months.

5 Enable Clear Options When Consent Is Required

When: If the personal data collected is sensitive, or that of a child.

Availability: Easily accessible on your website.

Method: Via a CMP.

6 Authenticate Consent for Collection of Sensitive Personal Data or Data From Minors

Sensitive personal data: Consent is required for processing [sensitive personal data](#).

Consent for children: Obtain consent from a parent or legal guardian for collection of personal data if the data subject is 13 or younger.

7 Consider Adopting a NIST-Aligned Privacy Program

Establishing and maintaining a written privacy program that conforms to the NIST Privacy Framework can serve as an affirmative defense against certain TIPA claims. This is a best practice, not a compliance requirement.

8 Enable Consumers to Make Data Subject Access Requests (DSARs)

Provide one or more contact options (e.g., toll-free phone number, web form, email). Set up a system to enable submission of [DSARs](#).

9 Set Up a System to Verify Data Subject Access Requests (DSARs)

As a best practice, enable consumers to attach documentation to help verify their identity and residency. If your business cannot reasonably verify a consumer's identity, inform them and explain why, and enable them to rectify.

10 Keep Track of Data Subject Access Requests (DSARs)

Set up a system to track all requests. Keep records of requests and responses for 2 years after the last consumer interaction.

11 Fulfill Data Subject Access Requests (DSARs)

Respond within 45 days from the date the request is received, extendable by an additional 45 days if the business notifies the consumer of the extension and its reason within that first 45-day window.

**Falling thresholds, rising enforcement and litigation,
eroding ad revenue. Do you know your risk?**

GET IN TOUCH